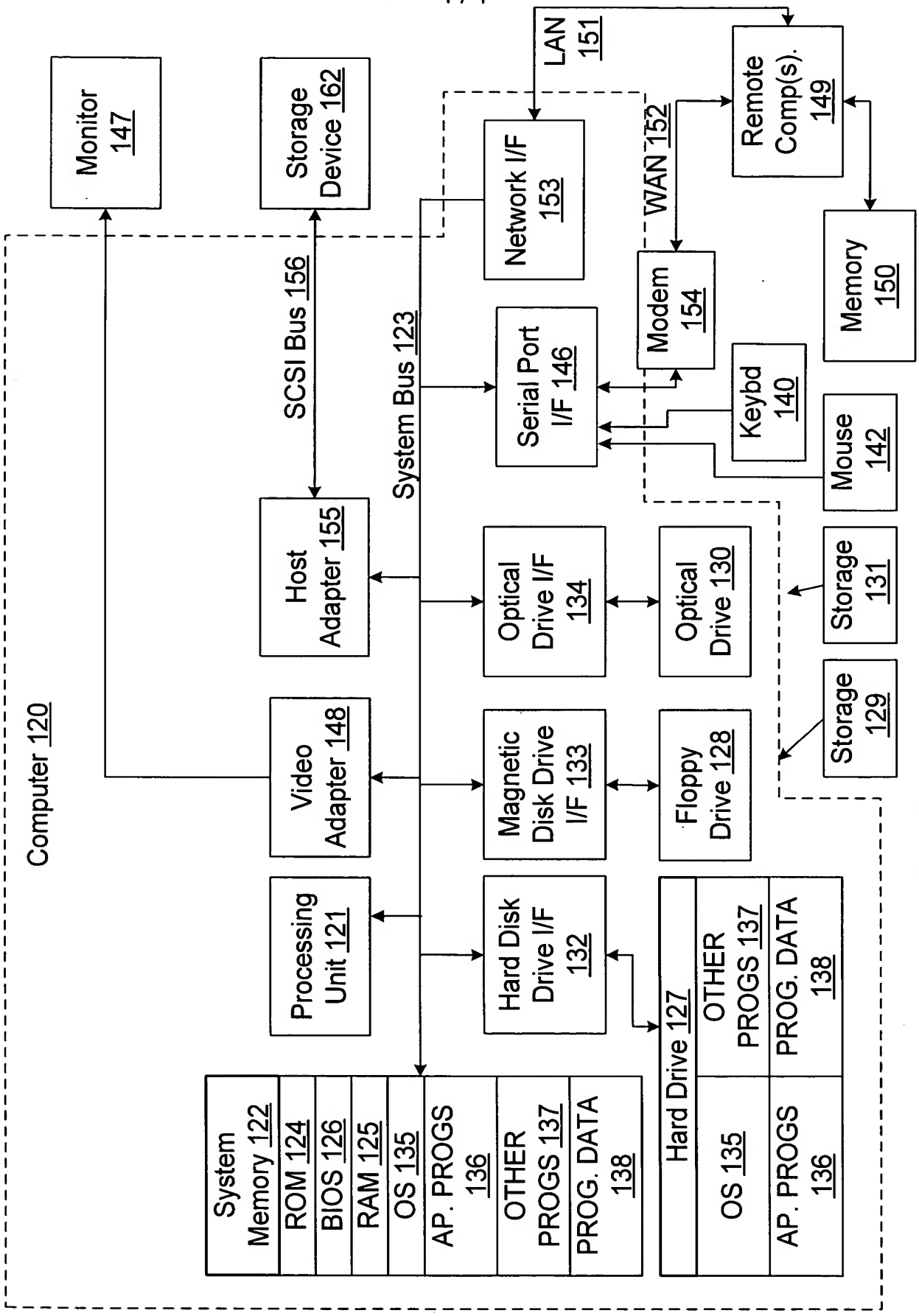
Computer 120
Monitor 147
Storage Device 162
LAN 151
Remote Comp(s). 149
Network I/F 153
WAN 152
Memory 150
Modem 154
SCSI Bus 156
System Bus 123
Serial Port I/F 146
Keybd 140
Mouse 142
Host Adapter 155
Optical Drive I/F 134
Optical Drive 130
Storage 131
Video Adapter 148
Magnetic Disk Drive I/F 133
Floppy Drive 128
Storage 129
Processing Unit 121
Hard Disk Drive I/F 132
System Memory 122
ROM 124
BIOS 126
RAM 125
OS 135
AP. PROGS 136
OTHER PROGS 137
PROG. DATA 138
Hard Drive 127
OS 135
AP. PROGS 136
OTHER PROGS 137
PROG. DATA 138

Fig. 1

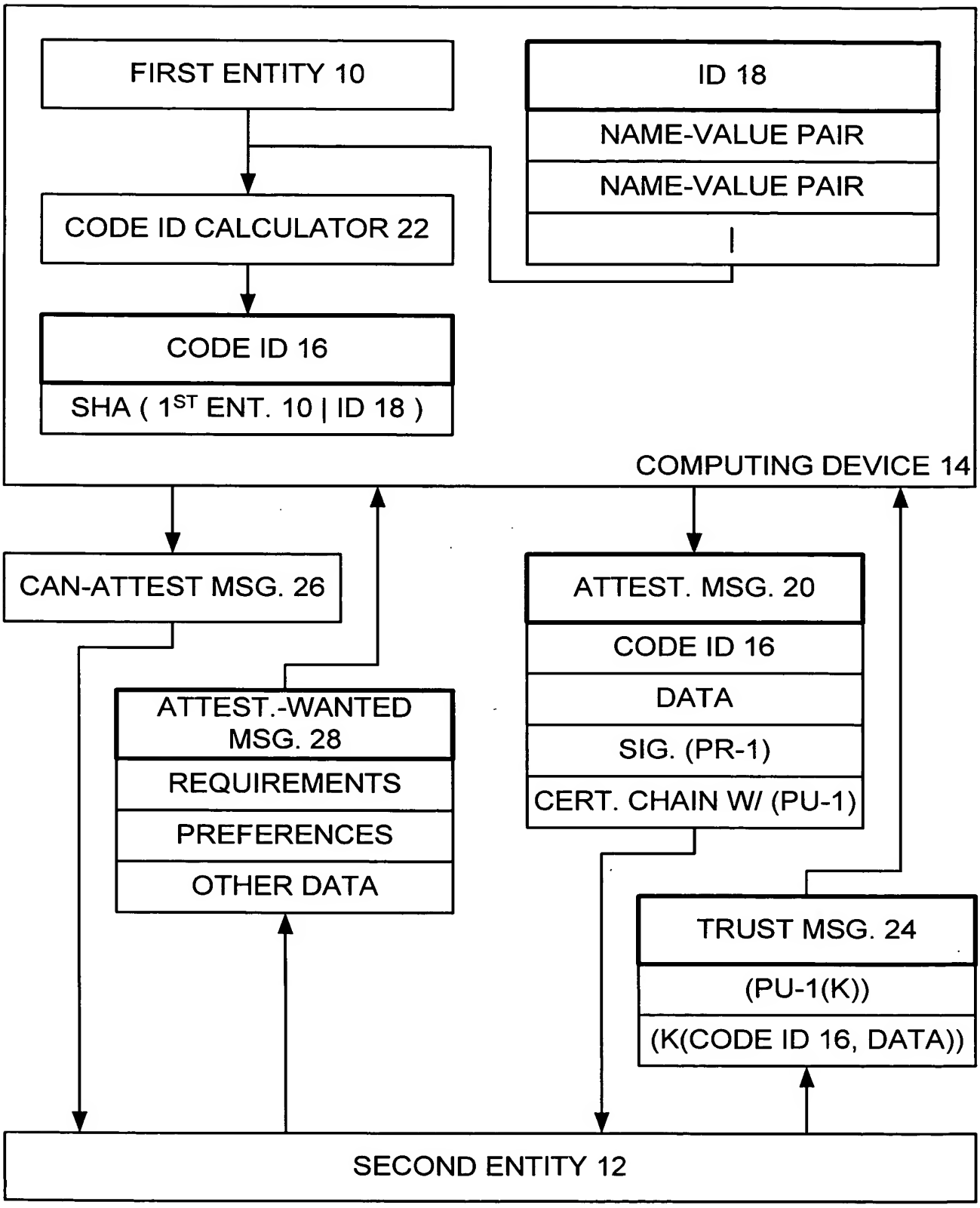
FIRST ENTITY 10
ID 18
NAME-VALUE PAIR
NAME-VALUE PAIR
CODE ID CALCULATOR 22
CODE ID 16
SHA (1ST ENT. 10 | ID 18)
COMPUTING DEVICE 14
CAN-ATTEST MSG. 26
ATTEST. MSG. 20
CODE ID 16
DATA
SIG. (PR-1)
CERT. CHAIN W/ (PU-1)
ATTEST.-WANTED MSG. 28
REQUIREMENTS
PREFERENCES
OTHER DATA
TRUST MSG. 24
(PU-1(K))
(K(CODE ID 16, DATA))
SECOND ENTITY 12

FIG. 2

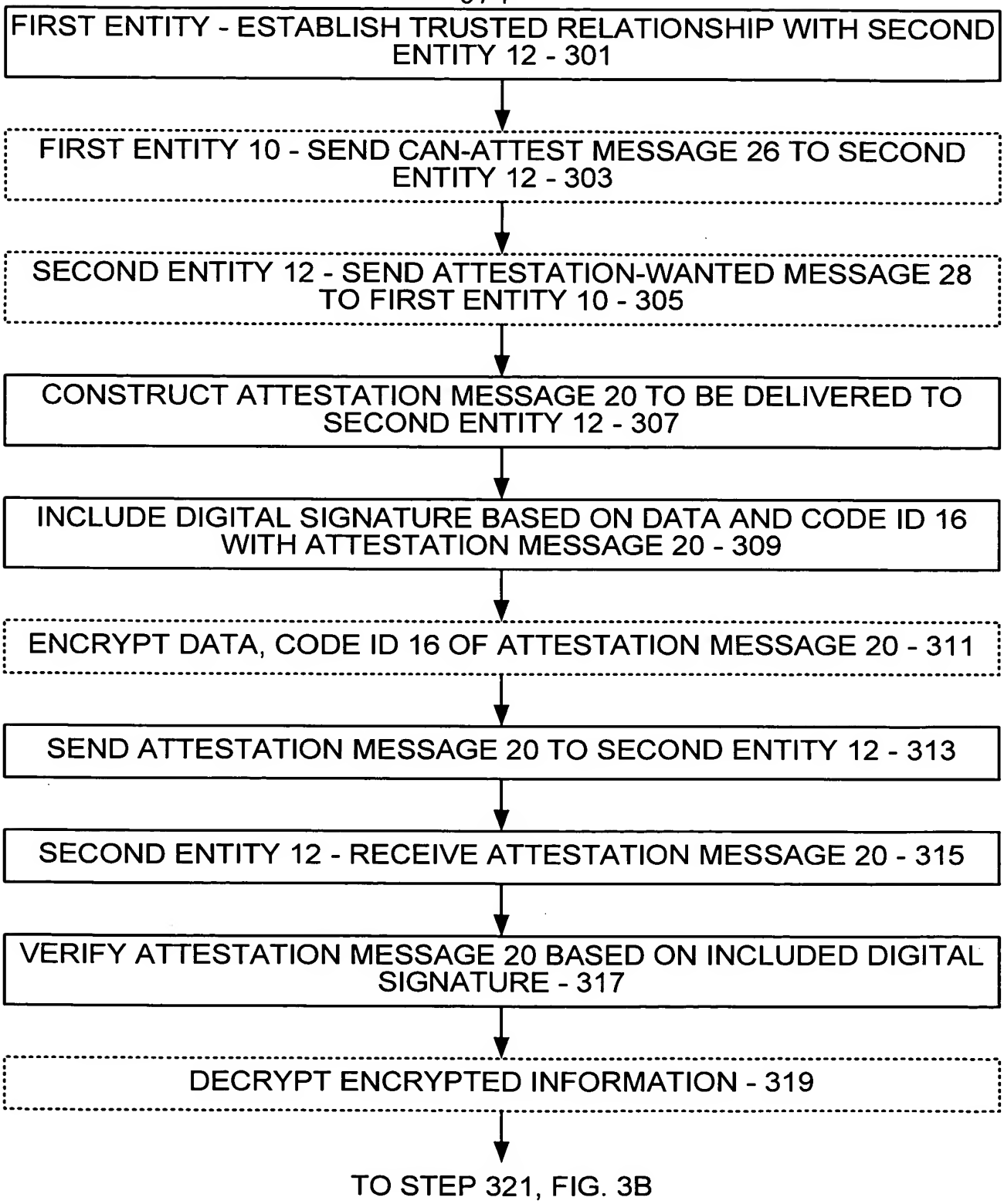
FIRST ENTITY - ESTABLISH TRUSTED RELATIONSHIP WITH SECOND ENTITY 12 - 301
FIRST ENTITY 10 - SEND CAN-ATTEST MESSAGE 26 TO SECOND ENTITY 12 - 303
SECOND ENTITY 12 - SEND ATTESTATION-WANTED MESSAGE 28 TO FIRST ENTITY 10 - 305
CONSTRUCT ATTESTATION MESSAGE 20 TO BE DELIVERED TO SECOND ENTITY 12 - 307
INCLUDE DIGITAL SIGNATURE BASED ON DATA AND CODE ID 16 WITH ATTESTATION MESSAGE 20 - 309
ENCRYPT DATA, CODE ID 16 OF ATTESTATION MESSAGE 20 - 311
SEND ATTESTATION MESSAGE 20 TO SECOND ENTITY 12 - 313
SECOND ENTITY 12 - RECEIVE ATTESTATION MESSAGE 20 - 315
VERIFY ATTESTATION MESSAGE 20 BASED ON INCLUDED DIGITAL SIGNATURE - 317
DECRYPT ENCRYPTED INFORMATION - 319
TO STEP 321, FIG. 3B

FIG. 3A

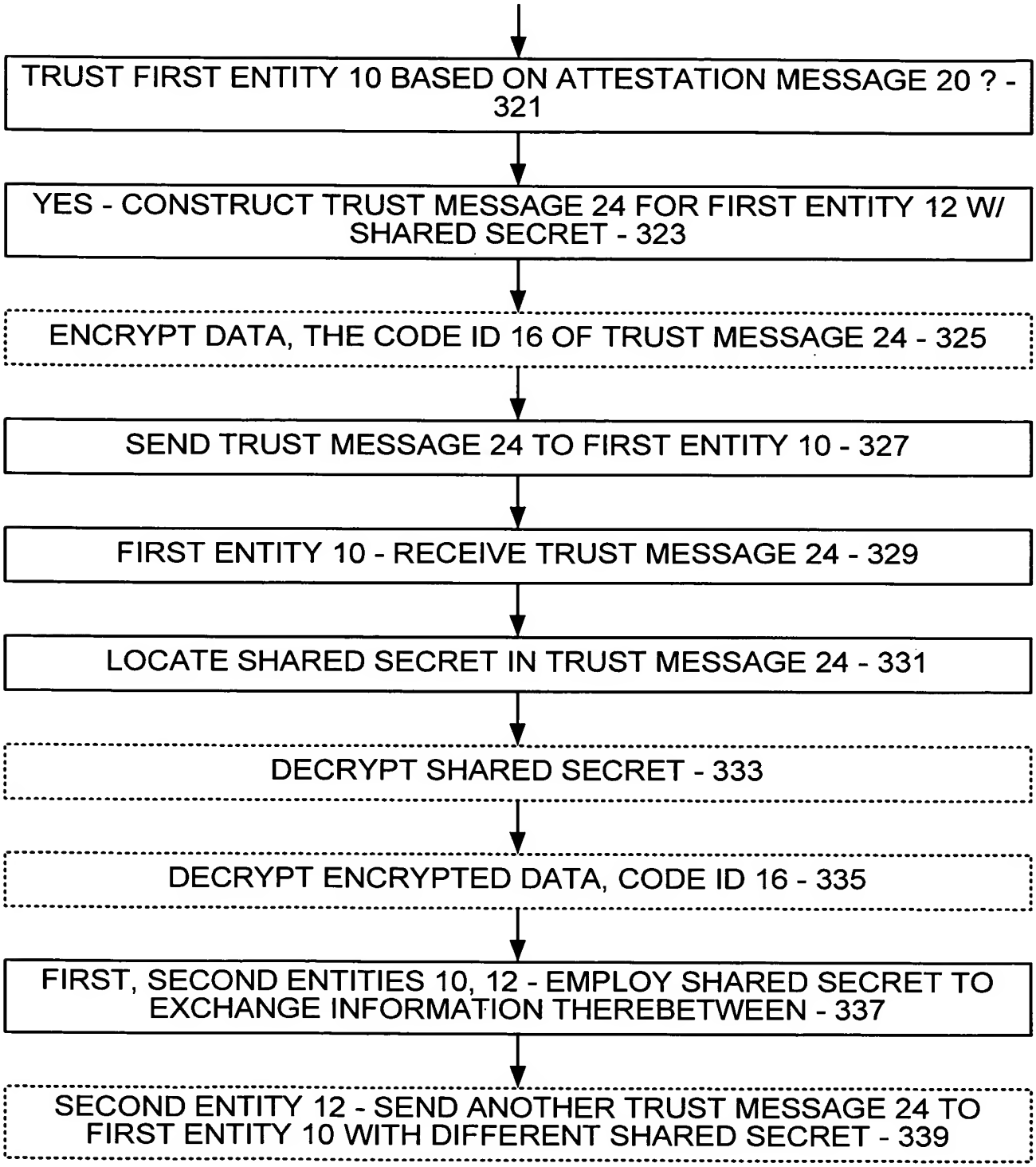
FROM STEP 319, FIG. 3A
TRUST FIRST ENTITY 10 BASED ON ATTESTATION MESSAGE 20 ? - 321
YES - CONSTRUCT TRUST MESSAGE 24 FOR FIRST ENTITY 12 W/ SHARED SECRET - 323
ENCRYPT DATA, THE CODE ID 16 OF TRUST MESSAGE 24 - 325
SEND TRUST MESSAGE 24 TO FIRST ENTITY 10 - 327
FIRST ENTITY 10 - RECEIVE TRUST MESSAGE 24 - 329
LOCATE SHARED SECRET IN TRUST MESSAGE 24 - 331
DECRYPT SHARED SECRET - 333
DECRYPT ENCRYPTED DATA, CODE ID 16 - 335
FIRST, SECOND ENTITIES 10, 12 - EMPLOY SHARED SECRET TO EXCHANGE INFORMATION THEREBETWEEN - 337
SECOND ENTITY 12 - SEND ANOTHER TRUST MESSAGE 24 TO FIRST ENTITY 10 WITH DIFFERENT SHARED SECRET - 339

FIG. 3B